

Programa del curso IC-8001

Criptografía

Escuela de Computación
Carrera de Ingeniería de Computación, Plan 410.

I parte: Aspectos relativos al plan de estudios

1 Datos generales

Nombre del curso:

Código:

IC-8001

Tipo de curso:

Teórico - Práctico

Nº de créditos:

4

Nº horas de clase por semana:

4

Nº horas extraclase por semana:

8

Ubicación en el plan de estudios:

Curso del 6° o 7° semestre de la carrera de Ingeniería en Computación

Requisitos:

MA1403 Matemática Discreta.

Correquisitos:

Ninguno

El curso es requisito de:

Ninguno

Asistencia:

Obligatoria

Suficiencia:

No

Posibilidad de reconocimiento:

No

Vigencia del programa:

I semestre 2016.

2 **Descripción** **general**

Curso teórico y formal que introduce al estudiante en el manejo de las técnicas computacionales de manejo de información con requerimientos altos de privacidad, así como a las técnicas para violentar esa privacidad, esto último con el afán de que sepan implementar prácticas sanas de incremento de la privacidad digital.

3 Objetivos **Objetivo General**

Objetivos Específicos

- Conocer las técnicas básicas para escribir buenos algoritmos de encriptación.
- Reconocer las características mínimas que debe poseer un protocolo de uso criptográfico seguro.
- Conocer las técnicas de ataque más utilizadas sobre la privacidad de las comunicaciones digitales.
- Conocer las funciones cuasi-criptográficas más empleadas para asegurar la autenticidad de los documentos digitales.

4 Contenidos 1. Introducción al Curso

- 1.1 Importancia de las técnicas de aseguramiento de la privacidad en las comunicaciones digitales
- 1.2 Conceptos básicos: el contexto de la criptografía
- 1.3 Teoría de la comunicación secreta de Shannon

2. Etapa pre-tecnológica

- 2.1 Sustitución
 - 2.1.1 Basada en “alfabetos”
 - 2.1.2 Sustitución de términos
 - 2.1.3 Códigos
- 2.2 Transposición: *Tabula recta*

3. Etapa tecnológica

- 3.1 Tecnología alemana: Enigma y máquina de Lorenz
 - 3.1.1 Funcionamiento de Enigma
 - 3.1.2 Funcionamiento de la máquina de Lorenz
 - 3.1.3 Criptoanálisis de Enigma
 - 3.1.4 Criptoanálisis de la máquina Lorenz
- 3.2 Algoritmos modernos
 - 3.2.1 El problema de distribución de la llave: algoritmo de Diffie-Helman
 - 3.2.2 Algoritmos simétricos (Llave privada)
 - 3.2.2.1 DES y TDES
 - 3.2.2.2 AES
 - 3.2.2.3 Twofish
 - 3.2.2.4 Blowfish
 - 3.2.3 Algoritmos asimétricos (Llave pública)
 - 3.2.3.1 RSA

- 3.2.3.2 El Gamal
 - 3.2.4 Criptografía cuántica
 - 3.2.5 Criptoanálisis moderno
 - 3.2.5.1 Fuerza bruta y poder computacional actual
 - 3.2.5.2 Man-in-the-middle
- 4 Algoritmos cuasi-criptográficos
 - 4.1 Funciones Hash criptográficas
 - 4.1.1 Conceptos Generales (MerkleDamgård)
 - 4.1.2 MD5
 - 4.1.3 SHA-1
 - 4.1.4 RIPEMD-128/256
 - 4.2 Block-chain
 - 4.2.1 Conceptos generales
 - 4.2.2 Aplicaciones
 - 4.3 Esteganografía
 - 4.3.1 Conceptos generales
 - 4.3.2 Esteganoanálisis
- 5 Ética de la implementación de la criptografía y el criptoanálisis

II parte: Aspectos operativos

5 Clases magistrales y proyectos.
Metodología de enseñanza y aprendizaje

6 Evaluación Asistencia y participación en clase. Asignaciones, exposiciones y afines.

Proyectos de investigación	20%
Proyectos programados grupales	80%
Total: 100%	

7 Bibliografía

+ : se usa en el curso
* : esta en la biblioteca
¡ : se puede comprar en librerías

El resto son libros de apoyo

(+*)Katz, J., & Lindell, Y. (2007). ***Introduction to modern cryptography: Principles and protocols*** (1era ed.). Boca Ratón, FL: Chapman and Hall/CRC.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). ***Handbook of applied cryptography (discrete mathematics and its applications)*** (1era ed.). Boca Ratón, FL: CRC Press.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). ***Security in computing*** (5ta ed.). Upper Saddle River, NJ: Prentice Hall.

(+*)Stallings, W. (2013). ***Cryptography and network security: Principles and practice*** (6ta ed.) Pearson.

8 Profesor

Ing. Jorge A. Vargas Calvo

Escuela de Computación, Oficina 19

Horas de Consulta: Martes a Viernes, de 2:00 PM a 3:00 PM

Se le recomienda al estudiante conocer el reglamento de enseñanza y aprendizaje del ITCR, en caso de fraude, apelación o conflicto el curso se registrará por dicho reglamento.

II parte: Aspectos operativos

4 Metodología de enseñanza y aprendizaje

- La metodología del curso consistirá en la impartición de clases magistrales por parte del profesor con la realización de actividades individuales por parte del estudiante como lecturas adicionales, investigaciones, trabajos escritos y experiencias de diseño y simulación de circuitos digitales. Habrá alternancia de virtuales y presenciales, y sesiones asincrónicas.
- Se tendrá disponible un grupo en la aplicación Telegram para atender las dudas de los estudiantes y para dar noticias importantes del curso, aunque el medio oficial de comunicación será el correo interno del ITCR, dirigido a las cuentas de correo de estudiante del ITCR. El enlace para unirse al grupo es <https://t.me/+IdQq94Nr3RE4NmUx>
- Las sesiones de consulta extra clase se llevarán a cabo mediante plataformas de interacción virtual (como Zoom, Google Meet, Microsoft Teams, etc.) y de manera presencial, en la oficina N°14 en la Escuela de Computación, los días en que hay clase presencial.
- La revisión de proyectos se llevará a cabo de manera virtual.
- El fraude, que consiste en presentar como propio trabajo realizado por otras personas (o por sistemas de asistencia electrónica) será calificado con un cero, y es susceptible de ser penalizado según la reglamentación vigente en el ITCR.
- Las sesiones presenciales tendrán lugar los siguientes días:
 - Julio: 26.
 - Agosto: 9, 23.
 - Septiembre: 6, 20.
 - Octubre: 4, 18, 25.
 - Noviembre: 1, 8.

- Si por alguna razón (religiosa, familiar, de salud, o de choque con otras actividades académicas) el estudiante no puede realizar alguna actividad calificada, esta se le podrá reponer mediante la presentación de la correspondiente justificación escrita.
- Las sesiones virtuales serán grabadas. Se dispondrá de un repositorio en One Drive para las mismas. La dirección de este repositorio es [IC8052 Criptografía](#)

5 Evaluación

- 2 exámenes parciales: 50%
- Proyectos de esquemas criptográficos: 30%
- Tareas: 20%

Total: 100%

- Las tareas serán escritas, en formato pdf, MS Word u Open Document. No se admitirá la fotografía o pdf de trabajos escritos a mano.
- Los exámenes parciales serán presenciales.